KOMOD

Konzeptstudie Mobilitätsdaten Österreich

ways2go

3. Projektbeiratssitzung: AP8 Datenschutz/E. Wolf

Mi, 25.05.2011, 9:30 – 14:00 Uhr

Moderation: Gerd Sammer, Institut für Verkehrswesen, BOKU

ways2go

bmvit

Bundesministerium
für Verkehr,
Innovation und Technologie

BOKU HERRY Verkehrsplanung / Consulting TU Graz salzburg research Karmasin Motivforschung WOLF

PROGRAMM

Arbeitspaket 8 Datenschutz (E. Wolf)

Bericht zu den Problemen der Erfassung und Bericht Leitfaden

- Grundproblem
- Was sind alles personenbezogene Daten?
- GPS-Daten
- Lösung bei GPS-Daten
- Zustimmungserklärung
- Zustimmungserklärung bei sensiblen Daten
- Anonymisierung (PAPI, CATI, CAWI)
- Pseudonymisierung
- Meldungen gem §§ 46 und 47
- Standardanwendung?
- Der Leitfaden

AP8 Datenschutz

Grundproblem:

Bei der Erfassung von Mobilitätsdaten werden personenbezogene Daten im Sinne des DSG ermittelt.
Daher ist das DSG 2000 igF anzuwenden.

Rechtsgrundlagen für KOMOD gem §6 Abs1 und §7 Abs1 DSG: §8 Abs 1 Z4 und Abs3 Z1; soweit sensible Daten erhoben werden: §9 Z10

AP8 Datenschutz

Zentrale Frage: Was sind personenbezogene Daten?

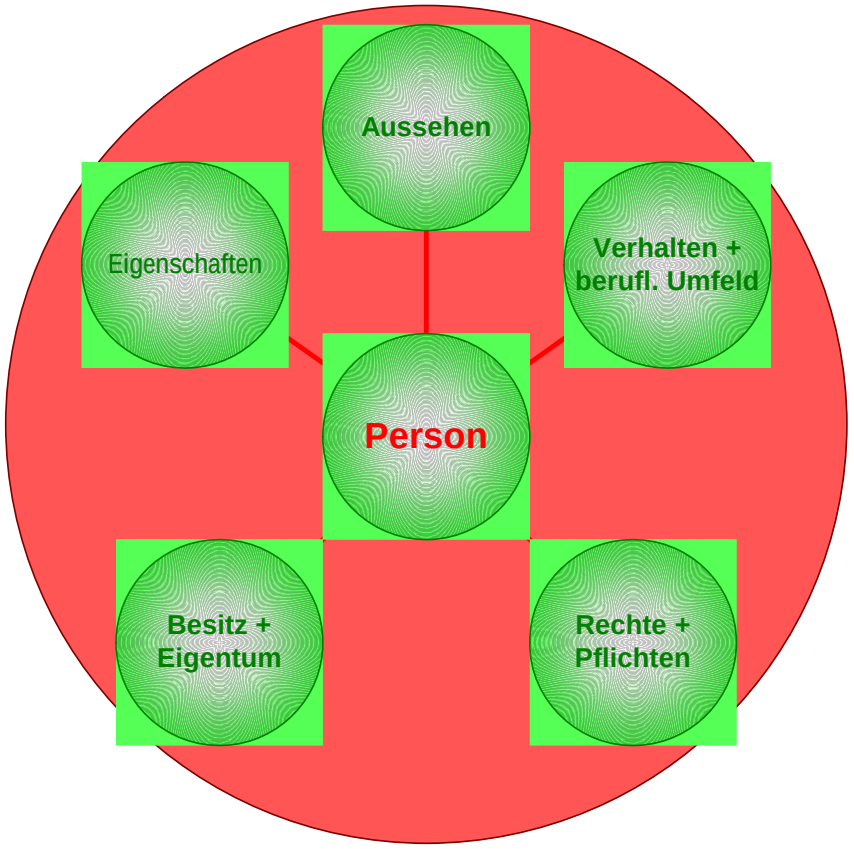
§4 Z1: Angaben über Betroffene (nat. Personen, jur. Personen u. Personengemeinschaften) deren Identität bestimmt oder mit legalen Mitteln bestimmbar ist.

Dazu gehören neben dem Namen und Adresse auch alle anderen Daten, mit Hilfe derer die Person identifizierbar wird.

Ein besonderes Problem entsteht durch Datamining-Methoden, weil dadurch aus mehreren (12- 15) anonymen Daten die Person rekonstruierbar wird.

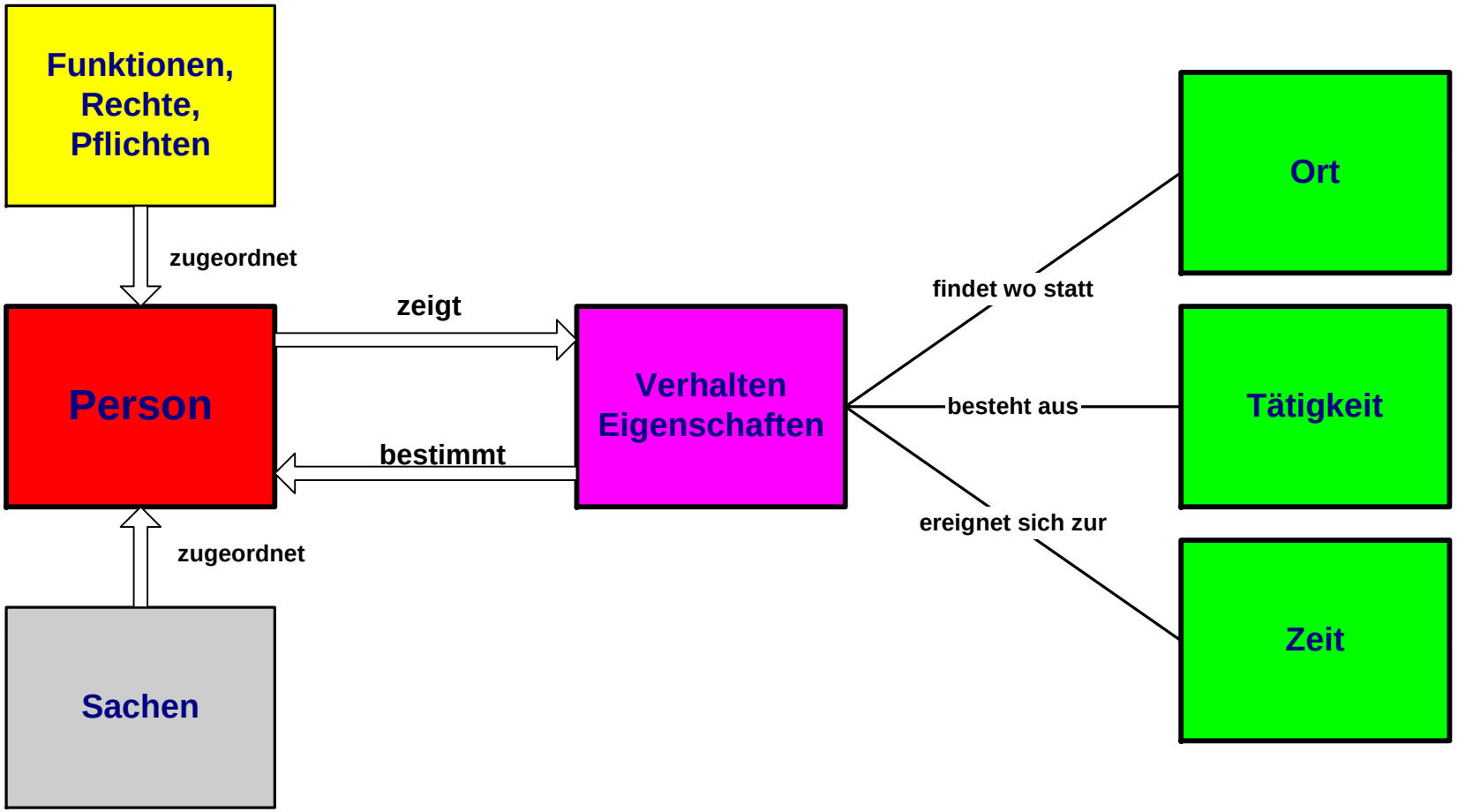
AP8 Datenschutz

Neben Name u. Adresse und den sonst geläufigen Daten einer Person kann man auf Grund des folgenden Bildes weitere Daten veranschaulichen:



AP8 Datenschutz

Aber es gibt noch weitere Möglichkeiten für identifizierende Daten:



AP8 Datenschutz

Ein besonderes Problem bilden **GPS-Daten**, weil durch sie auch bei Anonymisierung durch die genaue Position vor allem an **Anfangs- u. Endpunkten**, die Person identifizierbar wird, zB Anfangsort = Wohnung (Einfamilienhaus), Endpunkt = Arbeitsort (Geschäftslokal, Boutique usw). Aber durch **Zwischenorte** mit längerer Aufenthaltsdauer könnten **sogar sensible Daten** zu dieser Person entstehen (zB Verein, Kirche, Arzt, Spital, Parteilokal, Gewerkschaftslokal, Teilnahme an Demonstration, Bordell).

Solche Daten entstehen bei der Erfassung von Wegen mittels moderner **Smartphones** oder Ähnlichem. **Ausdrückliche Zustimmung des Trägers erforderlich,** wenn diese Daten auch verwendet werden sollen.

Nur bei **Mobilität von Behinderten** sinnvoll und dann **nach Aufklärung mit deren Zustimmung** verwendbar.

AP8 Datenschutz

Eine Lösung dieser GPS-Problematik:
Wenn nur Weglängen und Wegzeiten zu erfassen sind, dann entweder im Smartphone direkt oder bei Einlangen der Positionsdaten aus passiven GPS-Gerät in der Erfassungsstelle sofort wie folgt verarbeiten:
1. Weglänge zur Weiterverwendung aus Positionsdaten sofort berechnen und danach Positionsdaten sofort löschen, oder.
2. Weglänge zur Weiterverwendung aus Positionsdaten sofort berechnen und danach die Positionsdaten (GPS 5 Dezimalstellen) je nach Bedarf **letzten 2 oder 3 Dezimalstellen** runden und **Rest löschen**. Dadurch entsteht in unseren Breitengraden ein **Unbestimmtheitsbereich*)** von 750 bis 7,5 km Durchmesser. Dann können die Positionsdaten für ev. weitere Zwecke mit dieser Unbestimmtheit noch verwendet werden.

*) Erdradius R=6371 km, $U=2*\pi*R*\cos\varphi$, φ = 47,96 Grad Nord, 1° = 74,462km, 0,01° =745 m, 0,1° = 7,45km

AP8 Datenschutz

Zustimmungserklärung der befragten Person:
§4 Z14 schreibt vor, dass die Zustimmung zur Verwendung der Daten eine **gültige, ohne Zwang** abgegebene Willenserklärung des Betroffenen sein muss, die er in **Kenntnis der Sachlage für den konkreten Fall** erklärt (OGH 2Ob1/09z).

Das trifft für KOMOD dann zu, wenn Betroffener **volljährig** ist und **vorher** ausreichend über den
*** Zweck der Befragung,**
* die **Art der Verwendung** der Daten und
*** an wen übermittelt** wird,
*** samt Widerspruchsrecht**
klar und deutlich informiert wurde.

AP8 Datenschutz

Für die Zustimmungserklärung der befragten Person zur Verwendung **sensibler Daten** wird über §4 Z14 hinaus in **§9 Z6** verlangt, dass diese ausdrücklich erfolgen muss.

Das geschieht am besten und damit beweisbar in **Schriftform**.

Die Zustimmungserklärung zur Datenverwendung kann jederzeit widerrufen werden, was die Weiterverwendung der Daten unzulässig macht.
Der Widerruf ist nur möglich, wenn die Daten den Personenbezug aufweisen und gilt nicht für gesetzliche, gerichtliche oder vertragliche Datenverwendungen.

Bei Mobilitätsumfragen bei **PAPI** ist die Zustimmung **im ausgefüllten Fragebogen schriftlich vorliegend**, ebenso bei **CAWI**, aber **zweifelhaft und nicht beweisbar für sensible Daten bei CATI.**

AP8 Datenschutz

Die Verwendung personenbezogener Daten unterliegt dann nicht mehr dem DSG2000, wenn der Personenbezug nach Erfassung der Daten bleibend gelöscht wird => **Anonymisierung**! Damit entfallen auch alle Auskunfts- u. Widerrufsrechte des Betroffenen und das vereinfacht die Weiterbehandlung wesentlich. Das ist aber erst möglich, wenn der Befragte den Fragebogen (PAPI, CATI, CAWI) vollständig oder verwendbar ausgefüllt hat.

Bei **PAPI** sollte **nur das erste Blatt** die Koordinaten (Name, Adresse, Geburtsdatum, Telnr., E-Mail-Adresse) enthalten. Dieses **erste Blatt** wird nach der Erreichung der Vollständigkeit oder Verwendbarkeit des Fragebogens und Zuweisung eines Datensatzkennzeichens für den verbleibenden Datensatz **abgetrennt und bleibend vernichtet => Anonymisierung!**

AP8 Datenschutz

Bei **CATI** kann der Personenbezug im Datensatz entfallen, wenn im Erstinterview alle Daten erfasst werden. Das kann und soll dem Befragten auch mitgeteilt werden. Nur **wenn mehrere Interviews** notwendig, dann soll der Personenbezug im letzten Interview gelöscht werden.

Bei **CAWI** ist bei der letzten Kontrolle und **Entscheidung der Verwendbarkeit der Personenbezug bleibend zu löschen !**

Wenn der Personenbezug für irgend welche Gründe und Zwecke aufrecht bleiben soll, muss die **Pseudonymisierung** erfolgen, dh jeder Datensatz erhält anstatt des Namens ein Pseudonym oder eine Zufallszahl zugewiesen, die auch in der Personendatenbank aufbewahrt wird. Diese Personendatenbank wird getrennt und unter Verschluss aufbewahrt. Dadurch entstehen indirekt personenbezogene Daten, die gemäß dem DSG wesentlich erleichtert verarbeitet werden können.

AP8 Datenschutz

Meldungen gem §46 und §47 DSG:
Damit die im Rahmen von KOMOD vorgesehenen Mobilitätsbefragungen durchgeführt werden können, müssen entsprechende Anträge an die DSK gestellt werden. Öffentliche Daten gem §46 Abs 1 Z1 liegen in der notwendigen Qualität (Repräsentativität) idR nicht vor und auch indirekt personenbezogen Daten sind wegen der notwendigen Befragung nicht brauchbar.
Es verbleiben daher nur die bereits beim Auftraggeber vorhandenen Daten aus zulässigen früheren Befragungen oder neue Daten gem §46 Abs 2 und 3 und 3a und/oder §47 Abs3 Z3.

Die Verwendung neuer Daten (zB aus Melderegistern) stellt eine genehmigungspflichtige (durch die DSK) Übermittlung dar (§47 Abs3 Z3) und auch deren Verwendung (§47 Abs 4 u. 5) muss von der DSK genehmigt werden.

AP8 Datenschutz

Da diese Verfahren umständlich und bürokratisch ist, sollte das BMVIT überlegen, ob nicht eine Standardanwendung (SA036) beim BKA beantragt werden sollte, die solche Befragungen ohne den Umweg über die DSK gem §§46 und 47 erleichtert. Zugleich sollten in der Melde-VO auch die Kommunen berechtigt werden, für solche Umfragen entsprechende Meldedaten (als Auftraggeber der Umfragen) an die Dienstleister (die die Befragung durchführen) herauszugeben.

AP8 Datenschutz

Der Leitfaden zum Datenschutz im Verkehrswesen.

Beauftragt als Begleitstudie im Rahmen der 2. Ausschreibung ways2go
Projektziel: Anleitung der zukünftigen Projektleiter den Datenschutz von Anfang an einzuplanen nach dem **Prinzip „Privacy by Design“**

Besteht aus drei Teilen:
Kurzfassung in 10 Geboten des Datenschutzes (2 Seiten, 1 Blatt)
Langfassung mit ausführlichen Erklärungen der wichtigsten Begriffe und Anleitungen zur Durchführung des Schutzes in praktischen Beispielen (11 Mobilitätsuntersuchungen und 9 Intelligente Verkehrssysteme)
Technischer Leitfaden als Anhang zur praktischen Umsetzung des §14 DSG2000 und der ISO 27001-3

Nach Genehmigung und Freigabe durch BMVIT frei zum Herunterladen als farbiges PDF-File (in Summe ca. 200 Seiten).

AP8 Datenschutz

Vielen Dank für Ihre Aufmerksamkeit!
Diskussion und Fragen?